JPNT 14(4), 375-383 (2025)
https://doi.org/10.11003/JPNT.2025.14.4.375

JPNT Journal of Positioning, Navigation, and Timing

Zynq UltraScale+ RFSoC를 이용한 Multi-constellation GNSS 기만기 구현

박종일[1], 강창옥[1], 박일규[1], 박찬식[2†]

Implementation of Multi-constellation GNSS Spoofer Using Zynq UltraScale+ RFSoC

Jong-Il Park[1], Chang-Ok Kang[1], Il Kyu Park[1], Chansik Park[2†]
[1]Duksan Navcours Co. LTD, 66-6 Techno 2-ro, Yuseong-gu, Daejeon 34014, Korea
[2]Department of Intelligent System & Robotics, Chungbuk National University, Cheongju 28644, Korea

ABSTRACT

This paper presents the design and implementation of a multi-constellation Global Navigation Satellite System (GNSS) spoofer utilizing a multicore Asymmetric Multi-Processing (AMP) architecture based on the Zynq UltraScale+ RFSoC platform. The proposed system can simultaneously generate L1 band signals for GPS, GLONASS, and BeiDou and manipulate the target receiver's position solution in real time. For system implementation, three cores of the Cortex-A53 quad-core processor were operated in independent real-time OS environments, with each core performing signal generation parameter calculations for different constellations. The calculated parameters are shared through on-chip memory (OCM) and transferred to the signal generator in the programmable logic (PL) region for real-time GNSS signal synthesis. To achieve precise time synchronization between authentic GNSS signals and spoofing signals, the system delay time was measured and calibrated. The calibration results confirmed a time synchronization accuracy of 0.03 chips (approximately 30 ns) based on C/A code. Spoofing tests were conducted on a commercial GNSS receiver, the Septentrio SB3 Pro+. The results confirmed that the target receiver could be successfully spoofed to manipulate its position solution along an intended trajectory even in an environment where authentic GNSS signals and spoofing signals coexist.

Keywords: GNSS spoofing, multi-constellation, Zynq RFSoC, AMP
주요어: GNSS 기만, 다중 위성항법 시스템, Zynq RFSoC, AMP

1. 서론

Global Navigation Satellite System (GNSS)의 발전으로 인해 전세계 어디서나 고정밀 위치 정보와 정확한 시각을 손쉽게 확보할 수 있게 되었다. GNSS는 높은 정밀도와 개방된 접근성이라는 장점을 지니고 있어 항공, 해양, 농업 등 다양한 분야에서 널리 활용되고 있다 (Rumsfeld 2001, John 2001). 그러나 이렇게 누구나 이용 가능한 신호 구조와 낮은 신호전력은 GNSS의 치명적인 약점이 되기도 한다.

GNSS 신호는 수신기가 수신하는 과정에서 외부 전파 간섭이나 재밍 또는 기만 공격에 매우 취약하며, 공개된 프로토콜과 메시지 구조는 시스템의 신뢰성과 무결성에 부정적인 영향을 미칠 수 있다 (Warner & Johnston 2003, Humphreys et al. 2008). 특히 GNSS 신호를 모방해서 생성하는 기만 공격의 경우 수신기가 잘못된 위치해를 계산하게 하거나 시각 정보를 조작하는 것이 가능하다. 이는 GNSS를 기반으로 하는 시스템의 신뢰성과 무결성에 위협이 되며, 실제로 Unmanned Aerial Vehicle (UAV)나 자율주행 차량 등에서 심각한 문제를 발생시킬 수 있다 (John 2001, Warner & Johnston 2003, Humphreys et al. 2008).

이러한 GNSS의 구조적 취약성은 반대로 전쟁의 대응 기술로

Received Oct 20, 2025 **Revised** Nov 13, 2025 **Accepted** Nov 19, 2025

†**Corresponding Author** E-mail: chansp@cbnu.ac.kr

활용되고 있다. 이는 GNSS 신호를 사용하는 적군의 UAV나 정밀 유도 무기 시스템을 무력화하는 방식으로, GNSS 기만 기술이 전자전 장비의 형태로 운용되고 있다. 실제로 2011년도 12월에 미국 UAV가 이란 핵시설을 감시하다 GNSS 기만신호로 인해 탈취당한 사례를 발표한바가 있다 (Shepard et al. 2012a). 이후 시리아 내전 (C4ADS 2019)과 러시아-우크라이나 전쟁 (Lo et al. 2025)과 같은 분쟁지역에서도 GNSS 기만기를 활용하여 적 드론의 위치를 교란하거나 잘못된 경로로 유도함으로써 사전에 위협을 제거하거나 무력화하는 사례가 보고되고 있다. 또한 국내에서도 북한의 소행으로 판단되는 GNSS 기만신호로 인해 항공기 및 선박의 위치정보가 교란되는 사건도 있었다 (Goward 2024). 이외에도 GNSS 기만신호로 인한 피해는 지속적으로 발견되고 있다 (Scott 2017, Jones 2017).

이처럼 GNSS 기만이 실전에서 활용되는 사례가 보고되면서, 이를 가능하게 하는 장비인 GNSS 기만기에 대한 연구가 많아지고 있다 (Psiaki & Humphreys 2016). GNSS 기만기는 지금 현재 위치에서 보이는 GNSS 위성의 신호를 정밀하게 모방한 위조 GNSS 신호를 생성하여, GNSS 수신기가 잘못된 위치해나 시각 정보를 계산하도록 만드는 장비이다. 조금 더 응용된 GNSS 기만기의 경우 단순히 고정된 위치해를 교란하는 수준을 넘어, 도플러와 의사거리를 조작하여 수신기가 이동하는 경로를 계산하도록 유도하는 고도화된 GNSS 기만 기술도 연구되고 있다 (Kerns et al. 2014).

현재 GNSS 기만기는 주로 두 가지 방식으로 구현되고 있다. 첫 번째는 GNSS 시뮬레이터 기반 기만기로, Spirent (2024), Rohde & Schwarz (2025) 등의 상용 장비를 활용해 위성 궤도, 도플러, 시각 정보를 정밀하게 제어하며 multi-constellation 위성 시스템을 동시에 모사할 수 있다. 그러나 대부분 폐쇄형 구조로 되어 있어 구조적으로 수정이 어렵다. 또한 시뮬레이션 중간에 구성이나 경로를 바꾸는 실시간 제어가 어렵고, 장비가 매우 고가이며 렉마운트 형태로 되어있기 때문에 휴대성이 떨어진다는 단점이 있다. 두 번째는 Software Defined Radio (SDR) 기반 기만기로 HackRF (Margana et al. 2021), USRP (Altaweel et al. 2023) 등의 장비와 오픈소스 GNSS 신호 생성기를 이용해 저렴하게 구현할 수 있다. 이 방식은 구조 수정과 신호제어가 자유롭다는 장점이 있으나, 대부분 GPS L1 신호에만 한정되며 multi-constellation GNSS 시스템 구현에는 한계가 존재한다.

이러한 배경을 바탕으로, 본 논문에서는 Zynq UltraScale+ RFSoC 기반의 멀티코어 Asymmetric Multi-Processing (AMP) 구조를 활용해 현재 상공에 존재하는 multi-constellation GNSS를 동시에 모사하는 GNSS 기만기를 설계 및 구현한다.

이 논문의 구성은 다음과 같다. 2장에서 GNSS 기만기의 구조를 설명하고 Zynq UltraScale+ RFSoC를 이용한 multi-constellation GNSS 기만기의 구조 및 동작 방식에 대해 설명하였고, 3장에서는 구현한 GNSS 기만기의 성능을 상용 GNSS 수신기에 실제 GNSS 신호와 기만 신호를 동시에 송출함으로써 상용 GNSS 수신기의 결과 값의 변화를 확인하였다. 마지막으로 4장에서 결론 및 추후계획에 대해 서술하였다.

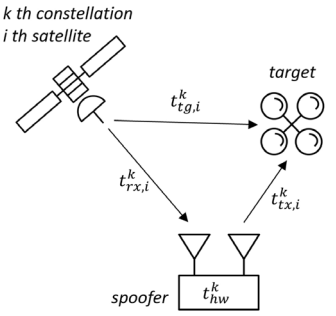

Fig. 1. Delay time components for time synchronization of GNSS spoofing signal.

2. 멀티코어 기반의 MULTI-CONSTELLATION GNSS 기만기

이 장에는 멀티코어 프로세싱을 활용한 multi-constellation GNSS 기만기의 설계 및 구현에 대해 설명한다. 먼저 GNSS 기만기의 기본 구조와 동작 원리를 살펴본 후, 이를 확장해 멀티코어 기반의 multi-constellation GNSS 기만기의 시스템 구성도를 제시한다. 제시한 시스템을 구현해 실제 GNSS 신호와 기만신호 사이에 얼마만큼의 지연이 발생했는지 constellation 별로 측정하고, 측정된 지연을 보상해 multi-constellation GNSS 기만기의 기만 정밀도를 향상시켰다.

2.1 GNSS 기만기의 구조

GNSS 신호는 크게 반송파, PRN 코드, 항법 메시지의 곱으로 구성된다. 특히, L1 대역 신호의 경우 ICD가 공개되어 있어 신호 구조가 알려져 있다. 알려진 신호 구조를 이용해 쉽게 GNSS 신호를 생성할 수 있다. 그러나 효과적인 GNSS 기만 신호 생성을 위해서는 단순히 반송파, PRN 코드, 항법 메시지를 일치시키는 것만으로 충분하지 않다 (Humphreys et al. 2008, Shepard & Humphreys 2011, Lee et al. 2022). 효과적으로 GNSS 기만 신호 생성을 하기 위해 목표 수신기의 안테나 위치에서 수신되는 시점의 신호 특성을 정밀하게 재현해야 한다. 이를 위해 전파 지연, 도플러 주파수와 같이 시간에 따라 변화하는 정보를 고려해야 한다. 이러한 정보가 고려된 GNSS 기만신호를 Eq. (1)과 같이 표현할 수 있다.

$$s_i^k(t) = A_i^k(t) d_i^k\left(t - t_i^k\right) c_i^k\left(t - t_i^k\right) \cos[2\pi(f_{IF}^k + f_{D,i}^k)t + \theta_i^k \quad (1)$$

여기서 $A_i^k(t)$는 constellation k의 i번째 위성의 신호 진폭을 나타내며, $d_i^k(t-t_i^k)$는 항법 메시지 데이터 비트를 나타낸다. $c_i^k(t-t_i^k)$는 위성의 고유 PRN 코드 시퀀스를 나타낸다. 여기서 t_i^k는 전파지연에 따른 코드 위상을 제어하기 위한 지연 파라미터이다. 지연 파라미터를 정밀하게 제어하면 목표 수신기의 위치 해를 GNSS 기만기가 설정한 위치해로 변경할 수 있다. 반송파 주파수의 f_{IF}^k는 GNSS 기만기 설계에 따라 constellation 별로 각각 다르며 $f_{D,i}^k$는 목표 수신기가 수신하는 위성별 도플러 주파수를 의미한다. $\theta_i^k(t)$는 시간에 따른 반송파 위상을 나타낸다. 특히 t_i^k는 GNSS 기만

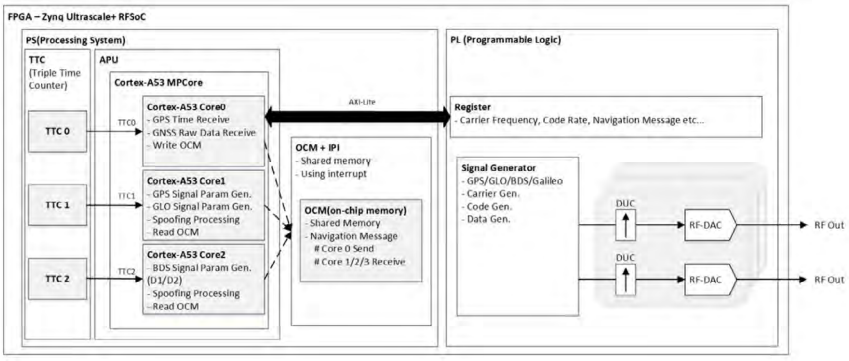

Fig. 2. Block diagram of multi-constellation GNSS spoofer system using multicore AMP structure.

성공률을 높여주는 중요한 파라미터로 C/A 코드의 칩을 기준으로 1칩 이내의 정확도를 가져야 목표 수신기를 의도된 위치로 잘못된 해를 계산하게 만들 수 있다 (Lee et al. 2022, Shepard et al. 2012c).

Fig. 1에서 보듯이, t_i^k는 k번 constellation의 i번째 위성으로부터 기만기의 수신안테나에는 $t_{rx,i}^k$ 시간이 목표 수신기의 안테나에는 $t_{tg,i}^k$의 지연된 시간으로 신호가 도착한다. 도착한 신호를 이용해 기만기가 생성을 시작하면, 생성된 기만신호는 기만기 내부 신호처리 지연 시간 t_{hw}^k와 목표 수신기까지의 전파 지연시간인 $t_{tx,i}^k$ 만큼 추가되어 목표 수신기에 도달하게 된다. 이러한 총 지연 시간인 t_i^k를 Eq. (2)와 같이 나타낼 수 있다 (Shepard et al. 2012b, Kerns et al. 2014).

$$t_i^k = t_{rx,i}^k - t_{tg,i}^k + t_{hw}^k + t_{tx,i}^k \tag{2}$$

지연 시간 계산식인 Eq. (2)에서 $t_{rx,i}^k, t_{tg,i}^k, t_{tx,i}^k$ 는 위성, 기만기, 목표 수신기 간의 기하학적 관계를 통해 계산할 수 있다. t_{hw}^k값은 각 constellation의 고유한 시스템 지연으로 신호생성시 신호처리에 의한 지연시간을 의미하는데 이는 신호처리를 수행하는 constellation 또는 하드웨어 마다 달라지는 경향이 있다. 시스템 지연인 t_{hw}^k를 측정하기 위해서 Park et al. (2023)이 사용한 다중상관기 기법을 사용했다. GNSS 수신기의 상관기 개수를 늘려 현재 신호추적 중인 신호뿐 만 아니라 주위에 생기는 기만신호까지 상관을 통해 신호유무를 파악할 수 있다. 기만 신호의 유무를 파악한 뒤 현재 추적 중인 신호와 기만신호 사이의 칩 간격을 통해 얼마나 지연이 생겼는지 확인할 수 있다. 얻은 지연 값인 $t_{rx,i}^k, t_{tg,i}^k, t_{tx,i}^k, t_{hw}^k$를 이용해서 최종적으로 t_i^k를 얻을 수 있다. 이를 통해 목표 수신기가 수신받는 GNSS 신호와 동일한 시각의 GNSS 기만신호를 생성할 수 있다.

2.2 Zynq UltraScale+ RFSoC를 이용한 Multi-constellation GNSS 기만기 설계

GNSS 기만기의 구조를 이용해 멀티코어 기반의 multi-constellation GNSS 기만기를 구현하기 위해 Xilinx사의 Zynq UltraSacle+ RFSoC ZCU28DR이 탑재된 ZCU111 보드를 하드웨어 플랫폼으로 선정했다. ZCU28DR RFSoC는 40 x 40 mm의 크기의 패키지로 제작되어 (XILINX 2020), ZCU28DR에 기만기를 설계하면 기존 시뮬레이터 기반의 GNSS 기만기의 단점인 크기와 중량 문제를 해소할 수 있다. 이러한 소형화 가능성을 실제 시스템으로 구현하고 검증하기 위해 ZCU28DR의 평가보드인 ZCU111을 활용해 multi-constellation GNSS 기만기를 설계했다 (Park et al. 2024).

ZCU111 보드는 통합형 RF 신호 처리에 관련된 아키텍처를 제공하며, 주요 구성요소는 다음과 같다. 첫째, RF-Analog to Digital Converter (ADC)와 RF-Digital to Analog Converter (DAC)가 각각 8개씩 내장되어 있어 별도의 외부 ADC/DAC 없이 사용자가 쉽게 RF 신호의 디지털 변환 및 생성이 가능하다. 본 시스템에서 다수의 RF-DAC를 이용해 각 constellation에 대해 병렬로 독립적으로 주파수 변조를 수행함으로써, 채널간 상호간섭을 최소화하고 주파수 계획 및 전력 제어의 유연성을 확보했다. 또한 시스템 복잡도를 감소시키고 신호 처리 지연시간을 최소화하는 장점을 갖고 있다. 둘째, Quad-core Arm Cortex-A53 기반의 Processing System (PS)가 탑재되어 있어 병렬처리 능력을 제공할 수 있다. 4개의 프로세싱 코어는 multi-constellation GNSS 신호 생성 시 요구되는 복잡한 연산을 효율적으로 분산 처리할 수 있도록 하였다.

이러한 ZCU111 보드의 구성요소를 이용해 Fig. 2와 같이 구성했다. 시스템은 크게 PS 와 Programmable Logic (PL) 영역으로 구분되어 동작하도록 설계하였다. PS 영역에서는 AMP 구조를 이용해 3개의 코어가 각각 real-time OS 환경에서 독립적으로 동작하게 구성하였다. Cortex-A53 쿼드코어 중 core0은 전체 시스템 관리와 제어를 담당하며, core1과 core2는 각각 constellation 별 신호 생성 파라미터 계산을 수행한다. Core3는 향후 Galileo 등 추가 constellation이 적용될 계획이어서 현재는 사용하지 않는다. GNSS 기만신호의 시각동기를 위해 Zynq 플랫폼에서 제공하는 전용 하드웨어 타이머인 Triple Timer Counter (TTC)를 활용했다. 코어 사이의 데이터 공유는 On-Chip Memory (OCM)를 사용했고, Inter-Processor Interrupt (IPI)를 이용해 데이터 처리를 즉각적으로 수행할 수 있도록 구성했다.

TTC는 100 MHz 클럭과 prescaler가 적용된 카운터 주파수로 동작하며, 각 코어들이 접근가능한 공통 시간기준을 제공하여 GNSS 신호 생성에 필요한 정밀한 시각 제어를 가능하게 한다. 정밀한 신호 생성 시각은 PL에 설정된 클럭과 GNSS 시각동기 수신기의 Pulse Per Second (PPS)를 기준으로 매초 보정해 결정된다.

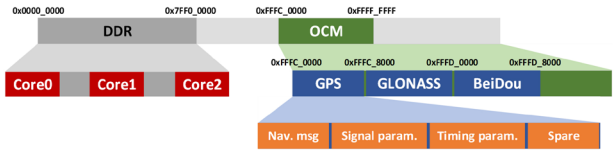

Fig. 3. Memory map of available memory regions in multi-constellation GNSS spoofer.

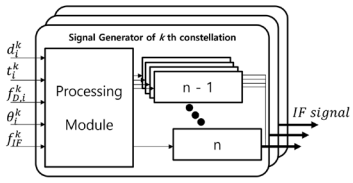

Fig. 4. GNSS signal generator structure in PL region.

Table 1. IF and NCO frequencies for multi-constellation GNSS signal generation.

Constellation	IF (MHz)	NCO (GHz)
GPS	75.42	1.5
GLONASS	75	1.527
BeiDou	75.098	1.486

OCM은 모든 코어가 접근 가능한 256 KB의 고속 공유 메모리로 실시간 파라미터 교환에 적합하며, Fig. 3과 같이 현재 시스템에 구현 중인 GPS, GLONASS, BeiDou constellation마다 OCM 영역을 나누어 사용하고 있다. 각 constellation은 32 KB 영역을 사용하고 있고 세부적으로 항법 메시지, 신호 파라미터, 시각 파라미터 정보를 주고받기 위해 사용 중이다.

IPI는 하드웨어 레벨에서 수십 ns 이내에 인터럽트를 전달하며, 인터럽트 처리 및 데이터 전송을 포함한 전체 통신 지연은 수 us 정도이다. 이는 현재 시스템의 신호 처리 주기 대비 충분히 작아 실시간 신호생성에 영향을 미치지 않는다. 신호 처리 주기마다 코어 간 즉각적인 동기화와 이벤트 통지를 가능하게 하여 multi-constellation 신호의 동시 생성에 필요한 정확한 타이밍 제어를 지원한다. 현재 동작하는 3개의 코어는 각기 다른 동작을 다음과 같이 수행한다. Cortex-A53 MPCore의 core0는 시스템 전체의 관리자 역할로서 OCM에 저장된 파라미터를 이용해 코어 및 데이터 관리를 수행하며, 신호생성에 필요한 정보를 Advanced eXtensible Interface (AXI) 버스를 통해 PL 영역으로 전달하는 중앙 제어 기능을 담당한다. core1은 GPS, GLONASS 신호 생성에 필요한 파라미터를, core2는 BeiDou 신호 생성에 필요한 파라미터를 계산하여 OCM에 저장해 PL영역으로 전달한다.

PL 영역에서는 PS의 core0에서 AXI 버스로 통해 전달받은 파라미터들을 이용해 GNSS 신호를 합성한다. 전달되는 파라미터는 Eq. (1)에 포함된 값들이며, 각 위성별 도플러 주파수, 항법 메시지, 시각정보 등의 파라미터 값을 PL의 Signal generator에 전달된다. Signal generator의 구조는 Fig. 4와 같이 구성되어 있다. 먼저 processing module에서 파라미터 값을 register에서 가져와 기만신호를 생성한다. 그 다음 n 개의 채널에 계산한 GNSS 신호와 동일한 도플러 주파수 오프셋을 갖는 IF 주파수와 PRN 코드를

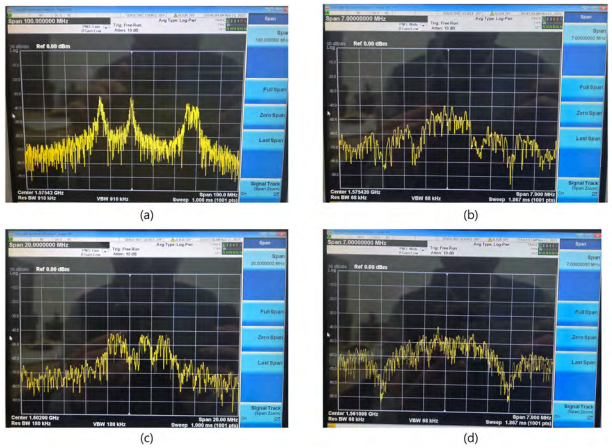

Fig. 5. Signal spectrum results of multi-constellation GNSS spoofer (a) center frequency: 1575.42 MHz, frequency span: 100 MHz (b) center frequency: 1575.42 MHz, frequency span: 7 MHz (c) center frequency: 1602 MHz, frequency span: 10 MHz (d) center frequency: 1561.098 MHz, frequency span: 7 MHz.

Table 2. FPGA resource utilization for multi-constellation GNSS spoofing system.

Resource	Available	Utilization
LUT	4525280	133226 (31.33%)
FF	850560	166518 (19.58%)
BRAM	1080	433.5 (40.14%)

생성한다. 그리고 얻은 지연시간을 이용해 코드의 위상을 결정한다. 코드 위상과 현재 시각을 이용해 송출할 항법 메시지를 결정한다. 이후로 생성된 신호의 코드 위상의 점차적인 변화로 목표 수신기의 항법해를 잘못된 해로 계산하게끔 만들 수 있다.

Processing module에서 생성된 n개의 위성신호는 합성되어 최종적으로 IF 신호로 출력되게 된다. 이는 현재 생성할 constellation의 개수에 맞게 병렬적으로 처리할 수 있도록 구성되었다. PL은 이러한 파라미터 정보들을 실시간으로 처리해 디지털 Intermediate Frequency (IF) 신호를 생성한다. 생성된 IF 신호는 각 constellation 별 설정에 따라 각각의 RF-DAC와 Digital Up-Converter (DUC)를 통해 병렬적으로 RF 신호로 변환되어 출력된다. DUC는 각 constellation 신호 별 주파수에 맞게 Table 1과 같이 설정하였고, Interpolation은 모두 8배로 설정했다. 제안하는 구조는 L1 대역의 각 constellation별 신호의 특성과 변조 방식을 사용해 GPS, GLONASS, BeiDou 신호를 Fig. 5a와 같이 동시에 생성할 수 있다. 최대 출력으로 신호를 생성한 결과로 -40 dBm의 세기를 갖고 있으며, 생성한 신호 외에 간섭신호가 생기지 않는 것을 확인했다. Fig. 5b는 GPS 신호를 확대한 결과로 GPS C/A code rate인 1.024 MHz의 2배인 약 2 MHz의 대역폭을 갖는다. Fig. 5c는 GLONASS 신호를 확대한 결과로 FDMA 특징인 채널별로 주파수가 다른 것을 확인했다. Fig. 5d는 BeiDou 신호를 확대한 결과로 BII code rate인 2.046 MHz의 2배인 약 4 MHz의 대역폭을 갖는다. Fig. 5를 통해 신호가 정상적으로 생성됨을 확인했다.

본 시스템의 PL 부분은 Vivado 2021.2에서 합성 및 구현되었으며, ZCU111 보드의 기준 리소스 사용률은 Table 2와 같다. PL

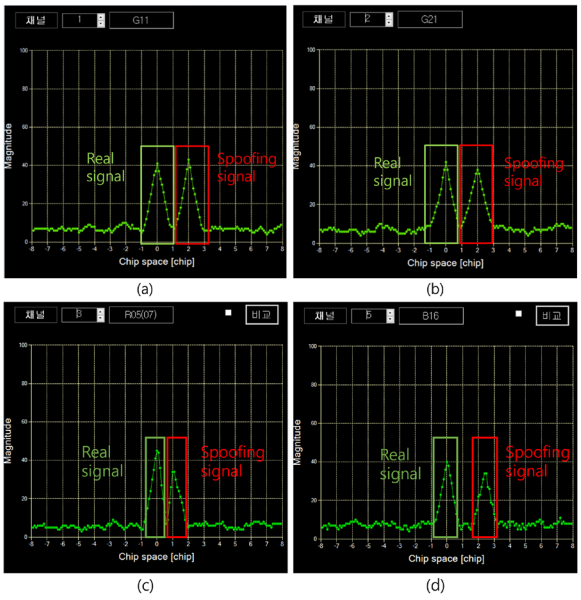

Fig. 6. System delay time measurement results (a) GPS PRN 11 satellite showing approximately 2 chip delay (b) GPS PRN 21 satellite showing approximately 2 chip delay (c) GLONASS channel number 5 satellite showing approximately 1.1 chip delay (d) BeiDou PRN 16 satellite showing approximately 2.4 chip delay.

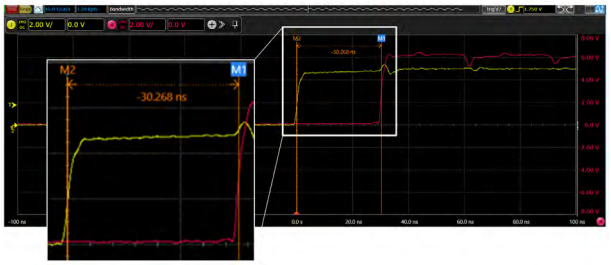

Fig. 7. 1PPS time synchronization measurement results showing 30.268 ns offset between authentic GNSS and spoofing signals.

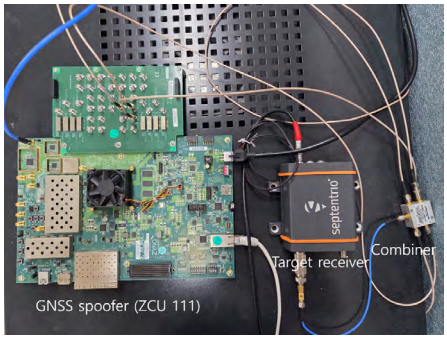

Fig. 8. Experimental setup for multi-constellation GNSS spoofing performance verification.

은 PRN 코드 생성 및 신호 제어 로직 중심으로 구현되어 주로 Look-Up Table (LUT) 기반의 신호 생성과, 신호 데이터 버퍼링을 위해 BRAM을 활용한다. Table 2에서 가장 많이 사용하고 있는 리소스는 BRAM이 40.14%를 사용하고 있으며, 현재 확인한 3개의 GPS, GLONASS, BeiDou 신호 이외에도 현재 미사용 중인 core3를 활용해 Galileo와 같은 추가 constellation 확장에 충분한 여유가 있는 것으로 확인된다.

2.3 지연시간 보정

GNSS 기만신호를 이용해 기만을 성공하기 위해서 목표 수신기에 맞는 지연시간 보정이 필요하다. 보정이 필요한 각 위성의 지연시간인 t_i^k를 측정하기 위해 네가지 지연요소 $t_{rx,i}^k, t_{tg,i}^k, t_{tx,i}^k, t_{hw}^k$ 를 획득해야 한다. $t_{rx,i}^k, t_{tg,i}^k, t_{tx,i}^k$은 현재 위성의 위치, 기만기의 위치, 목표 수신기의 위치를 각 위성의 ephemeris 정보와 위치해의 결과를 미리 측정해 얻을 수 있었다. t_{hw}^k는 Fig. 6과 같이 다중상관기를 이용해 측정했다. Fig. 6a는 GPS PRN 11 위성의 다중상관기 측정결과이고, Fig. 6b는 GPS PRN 21 위성의 다중상관기 측정결과이다. 이는, 다중상관기가 실제 GNSS 신호와 시각지연이 존재하는 기만신호를 동시에 수신할 경우 생기는 다중상관 결과이다. 일반적인 GNSS 수신기의 상관 결과는 1칩 이내에서 early (E), prompt (P), late (L)의 3개의 상관값을 이용해 현재 신호의 추적 상황을 보여준다. Fig. 6에서 보여주는 다중상관기에서는 16칩 구간을 0.1칩 간격으로 상관을 수행해 정밀하게 현재 신호의 상관 결과를 출력한다. 그래서 Fig. 6의 다중상관 결과를 통해 $t_{rx,i}^k, t_{tg,i}^k, t_{tx}^k$ 값이 모두 보정된 t_{hw}^k의 값을 얻을 수 있다. t_{hw}^k의 지연시각의 경우 시스템마다 다르기 때문에 GPS L1 C/A의 PRN 11, PRN 21의 위성의 t_{hw}^k가 약 2칩으로 일치함을 확인할 수 있다. 또한 다중상관기로 측정된 Fig. 6c의 GLONASS 지연시각인 1.1칩, Fig. 6d의 BeiDou 지연시각인 2.4칩을 시스템에 적용해야 한다.

3. GNSS 기만시험 및 결과

멀티코어 기반의 multi-constellation GNSS 기만신호의 성능을 확인하기 위해 2가지를 시험했다. 첫째 지연시간 정보인 t_i^k가 정확히 보정 되었는지 확인하기 위해 GNSS 시각동기 수신기를 이용해 실제 GNSS 신호와 기만신호의 지연시간 오차를 측정했다. 둘째 t_i^k를 보정해 생성한 신호를 이용해 실제 GNSS 신호와 기만신호를 동시에 상용수신기에 입력으로 넣었을 때 상용수신기에서의 기만동작을 확인했다.

첫번째 지연시간이 제대로 보정되었는지 확인하기 위해 2개의 GNSS 시각동기 수신기를 사용했다. 1개는 실제 GNSS 신호의 입력을 넣었고, 나머지 1개는 GNSS 기만기의 출력을 입력으로 넣었다. 각 GNSS 시각동기 수신기의 1PPS를 오실로스코프로 측정했다. 측정결과는 Fig. 7과 같이 30.268 ns 오차를 가지며 이는 C/A 코드 기준으로 약 0.03칩의 오차를 갖는다. 이는 Lee et al. (2022)에서 기준으로 제시한 1칩보다 정밀한 동기를 맞추고 있음을 확인했다.

두번째, 상용수신기에서 실제 GNSS 신호와 기만신호를 동시에 수신했을 때 기만 성능을 확인한다. 구성은 Fig. 8과 같이 GNSS 기만기가 구현된 ZCU111 보드와 기만신호의 목표가 될 상용수신기 그리고 실제 GNSS 신호와 기만신호를 합

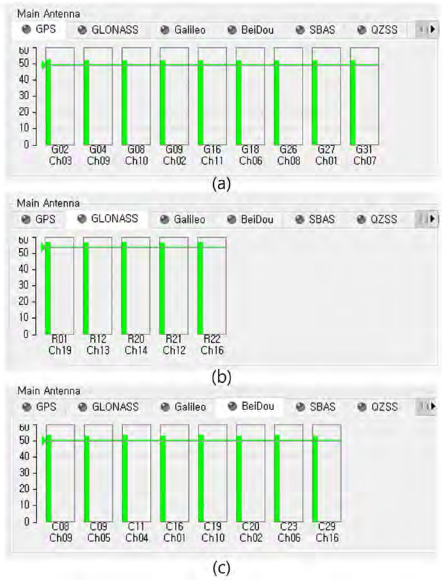

Fig. 9. Measured C/N_0 of multi-constellation GNSS spoofing signal. (a) GPS C/N_0, (b) GLONASS C/N_0, (c) BeiDou C/N_0.

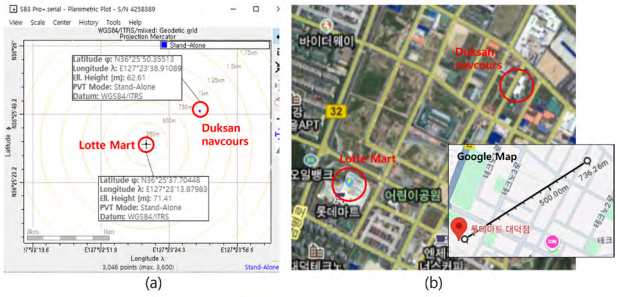

Fig. 10. Static scenario: position manipulation commands and target receiver position result (a) planimetric plot from Septentrio application (b) spoofing position setting in spoofing control application.

Fig. 11. Signal strength changes measured by commercial receiver during spoofing interval.

쳐줄 combiner로 되어있다. ZCU111 보드에서 L1 대역의 GPS, GLONASS, BeiDou 신호가 생성되고 이는 combiner로 연결된다. 목표 수신기는 상용수신기인 Septentrio SB3 pro+를 사용했다. Combiner는 총 4개의 신호를 하나로 합쳐주는 역할을 하며, 실제 GNSS 신호, 기만신호인 GPS, GLONASS, BeiDou 신호를 목표 수신기로 전달하는 역할을 수행한다.

시험은 static 기만과 dynamic 기만의 2가지 시나리오를 수행한다. 먼저 Static 기만 시나리오는 먼저 상용수신기에 실제 GNSS 신호만 입력으로 넣어주고, 상용수신기가 항법해를 계산한 결과를 확인한다. 그 후 상용수신기의 항기만 알고리즘을 회피하기 위해 실제 GNSS 신호를 끊고 10분 대기 후에 UI로 기만신호의 위치가 변경된 GNSS 기만신호를 입력으로 넣어준다. 기만신호의 위치는 덕산넵코어스 옥상을 기준으로 약 735 m 떨어진 롯데마트로 설정하였다.

먼저 Fig. 9는 Septentrio사에서 제공하는 어플리케이션을 이용하여 확인할 수 있는 위성별 C/N_0 그래프이다. Static 기만 신호를 출력했을 때 Fig. 9와 같이 총 22개 GPS, GLONASS, BeiDou의 기만신호를 생성했다. 세개의 constellation 모두 실제 GNSS 신호보다 10 dB 높게 신호를 생성했다. Fig. 9a의 GPS 위성의 C/N_0 값과 Fig. 9c에 보여지는 BeiDou 위성의 C/N_0 값이 모두 약 53 dB-Hz로 일치하는 것을 확인했고, Fig. 9b의 GLONASS 위성의 C/N_0 값은 약 56 dB-Hz로 일치하는 것을 확인했다. 같은 신호세기로 출력함에도 C/N_0 값이 GLONASS의 경우 GPS, BeiDou보다 약 3 dB-Hz로 높은데 이는 FDMA 특징으로 위성간 간섭이 CDMA보다 적어 생기는 현상으로 보인다.

Static 기만의 위치해 변경결과는 Fig. 10과 같은 결과를 얻었다. Fig. 10a는 Septentrio사에서 제공하는 어플리케이션을 이용해 출력한 위치해 결과이다. 중심의 위치해는 현재 GNSS 기만신호가 생성하는 롯데마트의 위치해를 나타내고, 2시 방향으로 약 740 m 떨어진 부분이 덕산넵코어스의 위치해이다. Fig. 10b는 위치해를 변경하는 UI의 일부와 Google 맵을 이용한 롯데마트와 덕산넵코어스 사이의 직선거리 값을 확인할 수 있다. Fig. 10a에서 보여주는 위치해의 Latitude-Longitude-Height (LLH) 좌표 값을 확인해보면 각각 롯데마트와 덕산넵코어스를 나타내는 것을 확인할 수 있으며, LLH 좌표를 데카르트 좌표계로 변환해 직선거리를 계산하면 약 735.46 m가 나오는 것을 확인했다. 이를 통해 UI에서 설정한 위치 값과 일치함을 확인하였다.

Dynamic 기만 시나리오는 먼저 상용수신기에 실제 GNSS 신호만 입력으로 넣어준다. 실제 GNSS 신호를 수신한 상용수신기가 Stand-Alone으로 항법해를 계산할 때까지 대기한다. 상용수신기의 항법해가 정상적으로 출력되는 것을 확인 후에 ZCU111 보드로 L1 대역의 GPS, GLONASS, BeiDou 기만신호를 실제 신호보다 10 dB 높게 생성한다. 초기 기만신호는 실제 GNSS 신호를 수신하는 안테나의 위치인 덕산넵코어스 옥상과 같은 위치의 항법해를 갖는다. 그 후 UI를 이용해 기만신호의 위치해를 변경했다. 변경방식은 덕산넵코어스 옥상을 기준으로 2시 방향으로 1 m/s씩 움직이도록 설정하였다.

먼저 Fig. 11은 Septentrio사에서 제공하는 RxControl 어플리케이션을 통해 출력한 C/N_0 값을 시간 축으로 표현한 그래프이다. 그래프에서 GPS, GLONASS, BeiDou의 C/N_0 값과 더불어 현재 위치해를 정상적으로 계산하고 있는지 아닌지를 PVT Mode 영역에서 확인할 수 있다. PVT Mode가 파란색일 경우 정상적으로 항

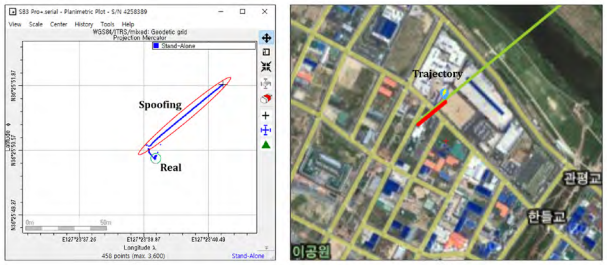

Fig. 12. Dynamic scenario: trajectory manipulation commands and target receiver position result changes (a) planimetric plot from Septentrio application (b) spoofing position setting in spoofing control application.

법해를 계산하는 중이고 빨간색일 경우 항법해를 계산하지 못하는 경우이다.

시험방식에 따라 초기에는 실제 GNSS 신호만 받아서 항법해를 수신하고 있다. 기만신호는 1:58:20에 출력을 시작해서 2:00:00에 기만신호의 위치해를 변경을 진행했으며 2:06:40에 출력을 중단했다. 시작 부분에서 C/N_0 값이 50 dB-Hz 이상으로 모두 증가한 것을 볼 수 있다. 이는 실제 GNSS보다 신호전력이 높은 기만신호를 수신했기 때문이다. 이를 통해 실제 GNSS 신호 대신에 기만신호를 수신하는 것을 확인할 수 있다. 기만신호를 수신하는 과정에서 1:58:20부터 2:00:00까지 C/N_0 값이 다른 시간대보다 심하게 변하는 것을 확인할 수 있는데, 이는 초기 기만 단계에서 실제 GNSS 신호와 기만신호가 동일한 위치에 공존하여 생기는 현상이다. 이 구간에서는 두 신호가 수신기의 추적 루프에서 경합하여 E, P, L의 상관 결과 값에 영향을 끼치는 것으로 판단된다. 특히 50 dB-Hz 이상의 높은 C/N_0 값은 기만신호가 실제 신호보다 약 10 dB 높은 전력으로 송출되었음을 나타낸다. 2:00:00 이후에 C/N_0는 안정적으로 변하는데, 이는 기만신호의 위치해를 변경함으로써 실제 GNSS의 지연시간과 기만신호의 지연시간의 차이가 Fig. 6과 유사하게 벌어지면서 생기는 현상으로 판단된다. 기만신호의 전력이 더 높기 때문에 목표 수신기는 점점 지연시각이 변경되는 기만신호를 추적하게 되고, 이로 인해 목표 수신기는 실제 GNSS 신호에 영향을 받지 않게 되면서 C/N_0 값이 안정적으로 변하게 된다. 기만신호 출력 중단시간인 2:06:40에 C/N_0 값이 실제 GNSS를 수신했을 때의 값으로 복구되는 것을 확인할 수 있다.

기만신호의 위치해 변경결과를 Fig. 12와 같이 확인했다. Fig. 12a는 Septentrio사에서 제공하는 어플리케이션을 통해 출력한 위치해 결과이다. Fig. 12b는 위치해를 변경하는 UI의 일부를 캡쳐한 그림이다. Fig. 12b의 초록색 선은 미리 계획된 기만 경로이며, 빨간색 선은 실시간으로 변경되는 현재 기만 위치를 나타낸다. 위치해 결과인 Fig. 12a는 Fig. 12b와 같이 계획된 기만 경로 방향인 2시 방향으로 위치해의 결과가 이동하는 것을 확인할 수 있었다. 이는 UI에서 설정한 위치해 변경 값과 일치하는 결과를 보여준다.

이러한 목표 상용수신기의 C/N_0 값과 위치해의 경로 이동의 결과는 실제 GNSS 신호와 기만신호의 0.03칩의 시각동기 정확도와 멀티코어 사이에 실시간 파라미터 업데이트가 효과적으로 작동했음을 보여준다.

4. 결론

Zynq UltraScale+ RFSoC 기반의 멀티코어 AMP 구조를 활용해 multi-constellation GNSS 기만기를 설계하고 구현했다. 제안된 시스템은 L1 대역의 GPS, GLONASS, BeiDou 신호를 동시에 생성할 수 있으며, 실시간으로 목표 수신기의 위치해를 조작할 수 있는 기능을 보여준다. 이 논문의 주요 성과는 다음과 같다. 멀티코어 AMP 구조를 통해 constellation별로 신호 생성을 독립적으로 처리함으로써 시스템의 확장성과 유연성을 확보했다. 또한 다중상관기 기법을 활용해 시스템 지연보정을 C/A 코드 기준으로 0.03칩 수준의 정밀한 시각을 보정했다. 이는 효과적인 기만공격에 필요한 1칩 이내의 시각오차를 만족한다. 구현된 GNSS 기만기는 상용 GNSS 수신기를 대상으로 한 실험에서 C/N_0 값을 통해 성공적으로 기만 성공을 확인했고, 위치해 결과를 통해 기만신호의 성공적인 위치해 조작을 확인하였다.

또한 Zynq UltraScale+ RFSoC를 이용한 multi-constellation 기만기의 기여는 SDR의 기반 기만기의 단일 constellation 지원 문제를 해결하고, 시뮬레이터 기반 기만기의 크기 문제를 개선했다. 특히 40 x 40 mm 패키지의 ZCU28DR RFSoC에 전체 시스템을 구현 가능함을 보임으로써 휴대용 multi-constellation GNSS 기만기의 실현가능성을 제시한다. 향후 연구 과제로 L2, L5 등 다중 주파수 대역의 확장과 Galileo를 포함한 추가 constellation 개발이 필요하다. 또한 더욱 정교한 기만 시나리오 구현을 위해 타겟의 위치해를 교란함으로써 원하는 위치로 이동시키는 유도 기만 알고리즘의 개발이 진행되어야 한다.

ACKNOWLEDGMENTS

본 연구는 다부처 사업으로 수행중인 불법드론 지능형 대응기술개발사업 (과제번호: 2021M3C4039579) 연구결과 중 일부임. 본 연구는 국방과학연구소(ADD)와의 선행연구를 기반으로 수행되었음 (912759101).

AUTHOR CONTRIBUTIONS

Conceptualization, J.-I.P. and C.-O.K.; Software, J.-I.P. and I.K.P.; FPGA Logic, C.-O.K.; Validation, J.-I.P.; Formal Analysis, J.-I.P.; Investigation, J.-I.P.; Resources, J.-I.P. and I.K.P.; Data Curation, J.-I.P.; Writing—Original Draft Preparation, J.-I.P.; Writing—Review and editing, J.-I.P., I.K.P. and C.P.; Visualization, J.-I.P.; Supervision, C.P.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Altaweel, A., Mukkath, H., & Kamel, I. 2023, GPS Spoofing Attacks in FANETs: A Systematic Literature Review, IEEE Access, 11, 55233-55280. https://doi.org/10.1109/ACCESS.2023.3281731

C4ADS 2019, Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria, Technical Report, Center for Advanced Defense Studies, Washington DC.

Goward, D. 2024, North Korea spoofing aircraft and ships [Internet], GPS World, 2024 Jun 3, available form: https://www.gpsworld.com/north-korea-spoofing-aircraft-and-ships/

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner Jr., P. M. 2008, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, In Proceedings of the 21st International technical meeting of the satellite division of the institute of navigation (ION GNSS 2008), Savannah, Georgia, 16-19 September 2008, pp.2314-2325. https://www.scirp.org/reference/referencespapers?referenceid=733459

John, A. Volpe National Transportation Systems Center (Volpe Center) 2001, Vulnerability Assessment of The Transportation Infrastructure Relying on The Global Positioning System

Jones, M. 2017, Spoofing in the Black Sea: What really happened? [Internet], GPS World, 2017 Oct 11, available form: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. 2014. Unmanned aircraft capture and control via GPS spoofing, Journal of field robotics, 31, 617-636. https://doi.org/10.1002/rob.21513

Lee, C. H., Choi, S. H., Lee Y. J., & Lee, S. J. 2022, Region Defense Technique Using Multiple Satellite Navigation Spoofing Signals, JPNT, 11, 173-179. https://doi.org/10.11003/JPNT.2022.11.3.173

Lo, S., Liu, Z., Ibrahim, L., Chen, Y. H., & Walter, T. 2025, Observations of GNSS Spoofing in Russia in 2023-2024. In Proceedings of the 2025 International Technical Meeting of The Institute of Navigation, Long Beach, California, 27-30 January 2025, pp.425-442. https://doi.org/10.33012/2025.19985

Margana, B. S., Achanta, D. S., Songala, K. K., & Ammana, S. R. 2021, A Simple SDR Based Method to Spoof Low-end GPS Aided Drones for Securing Locations, In 2021 IEEE International Conference on RAAICON, Dhaka, Bangladesh, 3-4 Dec 2021, pp.32-36. https://doi.org/10.1109/RAAICON54709.2021.9929965

Park, J. I., Lim, J. B., Kang, C. O., & Park, C. 2024, Development of Multi-constellation GNSS Spoofer Using Multicore-based AMP, In 2024 IPNT Conf., Phoenix Island Jeju, Korea, 6-8 Nov 2024, pp.163-166. https://www.ipnt.or.kr/2024proc/40

Park, J. I., Park, K. W., & Kang, C. O. 2023, Development of Multi-correlator Analysis Tool Using CUDA for Spoofing Signal Detection, In 2023 IPNT Conf., Shinhwa world Jeju, Korea, 1-3 Nov 2023, pp.241-244. https://www.ipnt.or.kr/2023proc/84

Psiaki, M. L. & Humphreys, T. E. 2016, GNSS Spoofing and Detection, Proceedings of the IEEE, 104, 1258-1270. https://doi.org/10.1109/JPROC.2016.2526658

Rohde & Schwarz 2025, GNSS and Avionics Simulation for Rohde & Schwarz Signal Generators, Version 17.00

Rumsfeld, D. H. 2001, Commission to Assess United States National Security Space Management and Organization, Committee on Armed Services of the US House of Representatives.

Scott, L. 2017, Spoofing Incident Report: An Illustration of Cascading Security Failure [Internet], Inside GNSS, 2017 Oct 9, available form: https://insidegnss.com/spoofing-incident-report-an-illustration-of-cascading-security-failure/

Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. 2012a, Drone Hack: Spoofing Attack Demonstration on a Civilian UAV [Internet], GPS World, 2012 Aug 1, available form: https://www.gpsworld.com/drone-hack/

Shepard, D. P., Bhatti, J. A., Humphreys, T. E., & Fansler, A. A. 2012b, Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks, In Proceedings of the 25th international technical meeting of the satellite division of the institute of navigation (ION GNSS 2012), Nashville, Tennessee, 17-21 Sep 2012, pp.3591-3605. https://www.ion.org/publications/abstract.cfm?articleID=10534

Shepard, D. P. & Humphreys, T. E. 2011, Characterization of Receiver Response to a Spoofing Attacks, In Proceedings of the 24th international technical meeting of the satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, Oregon, 20-23 Sep 2011, pp.2608-2618. https://www.ion.org/publications/abstract.cfm?articleID=9814

Shepard, D. P., Humphreys, T. E., & Fansler, A. A. 2012c, Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks, International Journal of Critical Infrastructure Protection, 5, 146-153. https://doi.org/10.1016/j.ijcip.2012.09.003

Spirent 2024, White paper: GNSS Signal Spoofing, DWP0014 Issue 1-02

Warner, J. S. & Johnston, R. G. 2003, GPS Spoofing

Countermeasures, Homeland Security Journal, 2, 19-27.
XILINX 2020, Zynq UltraScale+ Device Packaging and Pinouts: Product Specification User Guide, UG1075 (v1.9)

Jong-Il Park received B.S. and M.S. degrees from Chungbuk National University, Korea in 2018 and 2020, respectively. He has been research engineer of Duksan Navcours. His research interests include GNSS signal processing, GNSS, Drone, SDR and Spoofer.

Chang-Ok Kang received M.S. degrees from Hanbat National University in 2015. He is a Principal Research Engineer of Duksan Navcours. His research interests include Signal Processing Logic Design.

Il Kyu Park is a GNSS system engineer of Duksan Navcours Co., Ltd. He received B.S. and M.S. degrees completion in electronics engineering from Chungnam National University, Korea. He has been involved in several GNSS-related research projects: aerospace navigation system development, pseudolite system design and signal processing techniques. He is interested in the software GNSS receiver and simulation system development.

Chansik Park received B.S., M.S., and Ph.D. degrees in Electrical Engineering from Seoul National University in 1984, 1986 and 1997, respectively. He has been a Professor with the School of Electronics Engineering, Chungbuk National University, Cheongju, Korea, since 1997. His research interests include GNSS, PNS, SDR, integer ambiguity resolution algorithm and Error Analysis.